Published and Copyright (c) 1999 - 2016
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1838 09/23/16

~ More Clinton Mail Drama ~ People Are Talking! ~ ACLU and Snowden!
~ FCC Republicans Refusal ~ Super Pitfall Improved ~ Frogger Released!
~ Sega Gets Technosoft! ~ Israeli Pentagon DDoS ~ EU: Free Wi-Fi?

~ KrebsOnSecurity Silence ~ FBI Faking Hacks Is OK ~ New Twitter Rules

-* Atari’s Lunar Battle Mobile! *-
-* Blizzard Kills The Battle.net Brand *-
-* Yahoo Says Hack & Data Theft Was in 2014! *-

=~=~=~=

->From the Editor’s Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""

Summer is over, officially! The one thing that I will not miss from this past summer is the temperatures! There were almost 30 days in which the temperature reached at least 90 degrees in my area. And to make matters worse, we had very little rain. In fact, this was a record-setting summer for the least amount of rain! I’m hoping that fall-like weather continues beyond this weekend!

There’s enough "bad" news happening around the counry lately; I’m not going to comment because I’m sure that you’ve all probably been blitzed with it already. The only remark that I’ll make is that these events are disheartening. Even the tit-for-tat Trump and Clinton comedic campaigns can’t seem to bring many smiles these days! So, let’s just move right along!

Until next time...

=~=~=~=

Frogger - Released! STFM/E/TT030/Falcon

Frogger has been unleashed to the world.. get your copy here...

http://www.atarimania.com/game-atari-st-frogger_30782.html

I would like to take this opportunity to thank all those people that have helped me over the last 6 months... You know who you are ;)

Sys Reqs

1Mb STF/E TT030 / Falcon
Colour TV or RGB Mode
Jagpad / Keyboard / Joystick

Enjoy this game and let me get back to writing a new one :)

Some notes:
Read the instructions ;)
Although Frogger has been tested on the Falcon and TT and does indeed run, there may be graphical errors as the only access I have is Hatari (The latest Stable vers).

=~=~=~=

->In This Week's Gaming Section - Rise of Iron, A Tribute to Destiny!
""""""""""""""""""""""""""""""""" Blizzard Kills Battle.net Brand!
Sega Acquires Technosoft!
And much more!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
""""""""""""""""""""""""""""""""""""""

Rise of Iron Is A Heartfelt Tribute to The Last Two Years of Destiny

Rise of Iron is Destiny s fourth major expansion, and it plans for the game s future with new weapons, armor, missions, and multiplayer modes. It s as good an excuse as The Taken King was to jump back into developer Bungie s world: the loot is plentiful, the levels are easy to come by, and the sheer number of activities now available to players means the experience of upgrading your characters requires far less repetitive grind than it used to.

But that s not why I d recommend lapsed Destiny players play Rise of Iron. If, like me, you ve been playing Destiny off-and-on for more than two years, you should get Bungie s $30 DLC for one mission a mission that made me take my finger off the trigger for once, and actually look at the virtual world I d lived in for 643 hours of my life.

The mission s called We Found a Rifle, and (spoilers) it rewards players with an exotic Khvostov 7G-0X a fancified version of the very first gun players find in the game. On paper, the mission itself is an almost comedic distillation of Destiny s basic loop: use a gun to kill lots of baddies so you can get a better gun with which to kill more baddies faster. But in context, it s Bungie s tribute, both to the gun itself the only real way to express yourself in Destiny s world is through violence, and in that regard, the Khvostov was every Destiny player s first word and to the people who have spent hours, days, and weeks of their time in the game.

Destiny has made me satisfied, frustrated, excited, and bored

over the years I ve played it, but I felt a new emotion through this quest wistful. As I punched a four-eyed, four-armed vandal in the face so hard he turned purple and disappeared, I thought about how far Destiny had come in two years. As I hurled ethereal flaming hammers at a hovering metal eyeball, I thought about how far I had come in two years.

It s often difficult to quantify your real-world existence on this Earth, but by putting me back in Destiny s very first area with its very first gun, Rise of Iron cast it in stark terms: here was 26 months of my life measured in murdering video game monsters. I remembered waking up at ungodly hours to play acquaintances an ocean away, and mindlessly slaughtering dumb drones as an excuse to talk to an old friend. I could chart highs and lows in two years of my life by who I was killing that week.

My reflective mood was shared by Ghost: the little hovering robot that s been my constant companion in Destiny s world. The game s objectives are usually calls to action go here, hack that, kill them but the Khvostov mission s last request was simply to enjoy the view with Ghost.

 When you think about everything we've seen, everything we've done, the little robot said. I'll always remember our first day together. I realized then, that after so much time spent with Destiny, that I ll always remember it, too.

The Khvostov mission isn t the only time Rise of Iron gets caught in a reflective mood. The Plaguelands the expansion s new patrol area encompasses half of the Earth patrol area available at the game s launch. The familiar regions of the Rocketyard and the Divide have been tweaked, sliced, and scarred by nanobots belonging to new big bad SIVA, but they re still recognizable under a few extra feet of snow. I thought I d feel short-changed by this, given how many hours I ve spent on Destiny s Earth searching for spinmetal clusters, but the Plaguelands are still an intriguing treat: weirder than Venus, more bustling than Mars, and bigger than Oryx s Dreadnaught.

The story, too, is self-reflexive, but to its detriment. The short story missions in Rise of Iron rely on players caring about Destiny s version of ancient history: a group of proto-Guardians known as the Iron Lords who were killed generations before. I was getting misty-eyed at Ghost s request to take a moment together, but even I couldn t muster up much enthusiasm for the few missions on offer.

Destiny has been criticized for its flimsy plotline, the line I don t have time to explain why I don t have time to explain quoted as evidence of its wishy-washy sci-fi justification for shooting a lot of future guns. But Rise of Iron goes too far the other way. Quest gatekeeper Lord Saladin is over-earnest, humorless, and stiffed with lines that even hermit-living superhumans wouldn t say. After The Taken King injected some much-needed levity into the plot, Saladin draws it straight back out, and his attempts to maintain a sense of mystery fail a few missions in. Even the threat is underwhelming: SIVA s rogue nanobots have the potential to pull people apart at a molecular level, but Earth s greatest minds are happy sending one taciturn

Guardian and a really old dude in a furry collar to contain the threat.

But it s not those story missions that form the bulk of Rise of Iron. New three-player strike missions, multiplayer modes, and the Archon s Forge a public event space that pits players against waves of enemies are designed to be endlessly replayable. For existing players, Rise of Iron hides weeks worth of new missions, modes, and minor additions behind its weak story, as well as the promise of a new six-player raid coming this weekend. New Destiny players are getting even more of a deal.

At launch Destiny was a surprisingly slim package, but that problem s now been turned on its head. For new players, the game and its four expansions The Dark Below, House of Wolves, The Taken King, and now Rise of Iron are a daunting prospect. Destiny presents a solar system of game worlds filled with repeatable missions, events, patrols, strikes, dailies, heroics, raids, and other inscrutable options, like endless stars in the night sky. It s hard to tell Court of Oryx apart from the Archon s Forge, Prison of Elders from the Challenge of Elders, and the Vault of Glass raid from the Wrath of the Machine, but half of these activities spit out loot that s long obsolete.

But where previous Destiny expansions jettisoned what has come before, with wholesale tweaks to leveling, gear, and weapons, Rise of Iron builds on the sensible system introduced in The Taken King. Lapsed players can infuse armor and guns they particularly like, bringing treasured memories from Destiny s second year into its third, and the game s many vendors are happily handing over weapons that came to earn their own histories in the game s healthy community. I cheered out loud, for example, when I unpacked a brand-new Y-09 Longbow Synthesis last night with hidden hand and an ambush scope a set of words that mean nothing to normal people but will send a flicker of a smile across a Destiny player s face.

Almost every part of Rise of Iron combines old and new Destiny, from its weapons, to its leveling system, to its new patrol area. Two of its new strikes are even rehashes of the very first missions available to players, replacing some of the best-known bosses in the game with retooled, SIVA-infused versions of themselves. For the unsentimental, the casual fan, and the new player, that s not so important. If that s you, know that with the full Destiny collection you ll be getting a vast chunk of game for your $60, and know that you could also lose days, weeks, and months in its confines.

But for existing players, people for whom Destiny is already a hobby, people who get mild goosebumps when a video game robot tells you to take a moment, Rise of Iron is something special. It s a map for the future of Destiny, but it s also a wink and a nod at its past a chance for people who shared the route along the way to look back at where they ve come from.

Blizzard Kills The Classic Battle.net Brand After 20 Years

Blizzard is killing Battle.net just a few months shy of the online gaming service s 20th birthday killing the name, anyway. No, Overwatch and Hearthstone aren t going permanently offline or anything, you ll just be calling the service that hosts and updates your Blizzard games something else from now on.

In a post on its official forums, Blizzard announced that it is transitioning away from using the Battle.net name for our gaming service and the functionality connected to it. Instead, it ll use the considerably more boring convention where it just puts the name Blizzard in front of things, like Blizzard Streaming and Blizzard Voice. So presumably Battle.net will be Blizzard Gaming? Blizzard Launcher?

The reasoning is that back in 1996, when Battle.net was established (for the original Diablo good times) it was necessary to make it clear that this was a new and distinct online service. But over the years, confusion and inefficiencies apparently resulted from having a separate name for the service, and multiplayer is just an ordinary part of games these days, not something that requires separate branding.

Kind of true, but I still think this is a bad idea. Battle.net is an established and respected brand, known by gamers young and old. It s synonymous with online matchmaking and gaming I mean, it s right there in the name! Throwing away years of history like that is generally a bad idea, even when there are benefits to be had and I don t really see any benefits here. What if Steam was renamed Valve Store? Everyone would know Valve is behind it, sure, but you lose a household name in the process.

Well, there s no arguing with it. Blizzard has clearly made its decision and we re all going to have to call Battle.net something else soon.

We had some good times, Battle.net. RIP.

Sega Acquires Technosoft Franchises, Slowly Becoming Another Electronic Arts

Sega is a company that fans REALLY want to love and support but that love and support is more often than not met with lackluster Sonic the Hedgehog games. This bothers a lot of the gaming populace that remember Sega of old. The Sega that released Comix Zone, Streets of Rage 1, 2 and 3 on Sega Genesis, Shining the Holy Ark on Saturn, released the Dreamcast and more. For a lot of us it is apparent that that Sega is gone. Then they do things like acquiring the Technosoft library of games. If you are a retro gamer of any caliber then you know who Technosoft is. For the rest of you reading this, read on and prepare for a short history lesson.

Back in the day, Technosoft were one of THE developers of Sega Genesis games that every gamer had to have in their collection.

That is 100% true for their Thunder Force series of scrolling shooters. Thunder Force III and IV are arguably two of the best examples of the genre (TFIII was ported to SNES as Thunder Spirits - directly compared in our first issue). Technosoft was more than just the developer behind the Thunder Force series of games. They have also released Herzog Zwei and Elemental Master both also on the Sega Genesis console.

Technosoft s Thunder Force III was just announced to be coming to the Sega 3D Archives release. This is great news which hopefully means we will see Thunder Force IV, V and VI get HD remakes at some point (Thunder Force V was pretty awesome though IV is still my favorite).

Interestingly it is already confirmed that Sega is planning on re-releasing Thunder Force IV and V and Herzog Zwei at some point - platforms unknown at this time. Considering these were 16 and 32-Bit titles it could be just about any platform from the 3DS up to the Playstation 4 and Xbox One they are eyeing for these titles to hit. I am fine with that. Especially if they do remakes of some kind.

Atari s Lunar Battle, A New City-Builder and Space Shooter Coming to Mobile

Atari, one of the world s most recognized publishers and producers of interactive entertainment, today announced the development of Lunar Battle, a city-builder and space shooter coming soon to the App Store for iPhone, iPad, and iPod touch as well as on Google Play for Android devices in fall 2016. An original title, Lunar Battle crash lands players into an epic deep space adventure to explore uncharted terrain and conquer the skies. The free-to-play game incorporates arcade-style combat elements originally popularized in classic Atari space shooters such as Asteroids and Star Raiders into a base-building experience for mobile.

Beginning today, Lunar Battle has soft launched on the App Store and Google Play in Canada, Netherlands and Israel for a limited time before releasing worldwide.

Players will join the action as part of a brave crew of intergalactic explorers that crash-landed on a mysterious, inhospitable planet deep in space. Gathering resources and building infrastructure will be essential to ensuring the explorers can survive the desolate terrain and thrive into a growing populace. Protect the expanding base by taking to the skies to combat against AI and real-life opponents as part of the multiplayer experience. Become the ultimate ruler of the universe in Lunar Battle by mastering key gameplay features, including:

Build a Base Create a thriving planetary colony by building all the essentials a space community needs power, food, water, tech, beer and more. Customize building layouts to create the ultimate personalized galactic refuge.

Explore the Planet and Harvest Resources Unearth precious

resources including space ores, ship parts and energy sources. Use the materials to keep the population growing and colony thriving.

Take Flight and Fight Participate in PVE and PVP dogfights as part of the thrilling arcade space shooter experience. Use materials crafted and salvaged on the surface to outfit and upgrade space fighters with a selection of powerful lasers, plasma cannons, shields and more to become the terror of the nebula!

Destroy the Enemy Equip workers with blasters to fight off hordes of disgusting, deadly aliens and expand territory.

Conquer Campaigns Beat 50 levels of pulse-pounding space action. Try to score three stars on each level to receive rewards and salvage for completing missions.

Atari s history creating some of the most memorable arcade space shooters was the inspiration for Lunar Battle, said Fred Chesnais, Chief Executive Officer, Atari. The combination of our classic combat gameplay with a multiplayer experience and city-building simulation mechanics gives this all the makings of an engaging mobile game that will hook players and keep them coming back for deep space adventures again and again.

Lunar Battle is currently in development by On5. For more information, visit www.LunarBattle.com.

=~=~=~=

->A-ONE Gaming Online - Online Users Growl & Purr!

Fans Improve 8-Bit Nintendo Super Pitfall for 30th Anniversary

Most of the time when we cover retro game hacks here on Retro Gaming Magazine, it is usually to add a new character such as in Streets of Rage 2. Sometimes it is an improvement such as this one for Super Pitfall on the Nintendo Entertainment System. What fans have done here is almost create a new game, at least they did visually and aurally.

For those that don t know, Super Pitfall is a 2D side scrolling action platform game that expanded on the original formula of the Atari 2600 games. The levels were made bigger and longer, enemies are more varied and Super Pitfall is more engaging in general on the Nintendo NES.

Super Pitfall 30th Anniversary Edition is still the classic game, just now the graphics and music have been improved beyond what was formerly though possible on the 8-Bit Nintendo Entertainment System. I mean, just look at the comparison shots below there. That is an IMPROVEMENT and a half if I have ever seen one.

Not just gussied up graphics and music have found their way into

Super Pitfall 30th Anniversary Edition though. Nope, the fans behind this hack have also added new menu screens, improved the game level design a bit by removing unnecessary warps and hidden items. Hardcore fans of Super Pitfall will probably notice a bit of a performance improvement in this hack also. There is also a fully automatic save feature included, at no extra charge. Who wishes that some role playing games on the Nintendo Entertainment System included a seamless automatic save feature? I know I do.

As usual, we here at Retro Gaming Magazine do not condone piracy and all of that jazz. For those that want the patch head over to ROMHacking.net and grab it. We cannot link to a site to get Super Pitfall as it is not freeware. If you enjoy this hack, please remember to leave a comment on ROMHacking.net saying so, the developers will appreciate it.

Global Game Gear Asks How Are You Protecting Your Atari 2600 Collection?

It is an age old question. How to protect your gaming library. Sure, there were some companies that provided protective sleeves for some of their titles. Nintendo did this for pretty much all of the NES games that were officially licensed. They also did this for some of the Super Nintendo games they released - eventually opting to drop the little plastic sleeve (many experts \state that this move saved Nintendo a nickel per game). That is all find and dandy if you still have those sleeves. For most gamers buying titles loose, or used, those slip covers are LONG gone. There are aftermarket options for SNES and others but what about the Atari 2600? Atari never really addressed this issue. Global Game Gear is stepping up and doing it for Atari- over 30 years later.

The protective covers that Global Game Gear are working to produce are dusted and somewhat transparent. This allows protection to the cartridge and label but still lets you see some of the original artwork on the cartridge. That is what this is really about, at least for me. Some of those Atari 2600 games had amazing cover art on them. A completely opaque dust cover would simply not work as that would block all of the artwork and that would be a crime in my eyes.

Okay, let s get down to cost here. At the lowest pledge to actually receive Global Game Gear dust covers for your Atari 2600 retro games you are going to get 10 units. This pledge is at $15, which is about $1.50 per dust cover. I know, for a lot of us that is more than we paid for the games we are putting into the dust cover. For others, 10 units may not be enough. Pledge at the highest level, $500, and you get 519 dust covers - this level gives the most value, obviously but also the highest out of pocket cost. At the $500 level, the Global Game Gear dust covers are priced at just a hair above $0.96 each. This level is for the hardcore collector that understands as time goes on getting mint condition cartridges is going to eventually become a valuable commodity.

So, how are you protecting your Atari 2600 retro gaming library? If you don t have a solution and want one, here you go. I can easily see collectors with valuable games opting for Global Game Gear protective sleeves. If that is you then head over to their Kickstarter and pledge.

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Yahoo Says Hackers Stole Data from 500 Million Accounts in 2014

Yahoo Inc said on Thursday that at least 500 million of its accounts were hacked in 2014 by what it believed was a state-sponsored actor, a theft that appeared to be the world's biggest known cyber breach by far.

Cyber thieves may have stolen names, email addresses, telephone numbers, dates of birth and encrypted passwords, the company said. But unprotected passwords, payment card data and bank account information did not appear to have been compromised, signalling that some of the most valuable user data was not taken.

The attack on Yahoo was unprecedented in size, more than triple other large attacks on sites such as eBay Inc , and it comes to light at a difficult time for Yahoo.

Chief Executive Officer Marissa Mayer is under pressure to shore up the flagging fortunes of the site founded in 1994, and the company in July agreed to a $4.83 billion cash sale of its internet business to Verizon Communications Inc .

"This is the biggest data breach ever," said well-known cryptologist Bruce Schneier, adding that the impact on Yahoo and its users remained unclear because many questions remain, including the identity of the state-sponsored hackers behind it.

On its website on Thursday, Yahoo encouraged users to change their passwords but did not require it.

Although the attack happened in 2014, Yahoo only discovered the incursion after August reports of a separate breach. While that report turned out to be false, Yahoo's investigation turned up the 2014 theft, according to a person familiar with the matter.

Analyst Robert Peck of SunTrust Robinson Humphrey said the breach probably was not enough to prompt Verizon to abandon its deal with Yahoo, but it could call for a price decrease of $100 million to $200 million, depending on how many users leave Yahoo.

Steven Caponi, an attorney at K&L Gates with a practice including merger litigation, said that Yahoo’s breach could fall under the "material adverse change" clause common in mergers allowing a buyer to walk away if its target’s value deteriorates.

"That would give Verizon the opportunity to renegotiate the terms or potentially walk away from the transaction if it is a material change. Whether it is a material change will depend in large part on what kind of information was compromised," Caponi said.

Still, it is rare for mergers to fall apart over material changes. Verizon said in a statement it was made aware of the breach within the last two days and had limited information about the matter.

"We will evaluate as the investigation continues through the lens of overall Verizon interests," the company said.

Shares of Yahoo stock closed a penny higher at $44.15, while shares of Verizon, were up about 1 percent.

The Yahoo breach follows a rising number of other large-scale data attacks and could make it a watershed event that prompts government and businesses to put more effort into bolstering defences, said Dan Kaminsky, a well-known internet security expert.

Retailers and health insurers have been especially hard hit after high-profile breaches at Home Depot Inc , Target Corp, Anthem Inc and Premera Blue Cross.

"Five hundred of the Fortune 500 have been hacked," he said. "If anything has changed, it’s that these attacks are getting publicly disclosed."

Three U.S. intelligence officials, who declined to be identified by name, said they believed the attack was state-sponsored because of its resemblance to previous hacks traced to Russian intelligence agencies or hackers acting at their direction.

Yahoo said it was working with law enforcement on the matter, and the FBI said it was investigating.

"The investigation has found no evidence that the state-sponsored actor is currently in Yahoo’s network," the company said.

While the breach comprised mostly low-value information, it did include security questions and answers created by users themselves. That data could make users vulnerable if they use the same answers on other sites.

A former Yahoo employee said the Q&A were deliberately left unencrypted, which allowed Yahoo to catch fake accounts more easily because fake accounts tended to reuse questions and answers.

News of the massive breach at one of the nation’s largest email providers may fan concern that U.S. companies and government

agencies are not doing enough to improve cyber security.

Democratic Senator Mark Warner said in a statement he was "most troubled by news that this breach occurred in 2014, and yet the public is only learning details of it today."

Technology website Recode first reported Tuesday that Yahoo planned to disclose details about a data breach affecting hundreds of millions of users.

House Panel Looking into Reddit Post Linked to Clinton s Deleted Email

Paul Combetta, the IT guy who reportedly deleted Hillary Clinton s emails despite Congress orders to preserve them, was given immunity by the Department of Justice a few weeks ago.

Republicans wanted those email deletions investigated, but Combetta s immunity deal made that prospect unlikely, the New York Times reported earlier this month.

It s just gotten more than likely: in fact, a House panel is now looking into a Reddit post asking for help in how to delete email, The Hill reports.

The investigation was sparked after an army of Redditor investigators found what they consider a smoking gun: a user with the handle of stonetear who 2 years ago submitted a request for advice on how to strip out a VERY VIP email address from a bunch of archived email.

Combetta is an engineer with Platte River Networks, the firm that managed Clinton s private server.

He s currently one of the targets of a broader Oversight investigation on whether Clinton ordered the destruction of emails that had been subpoenaed by the Benghazi Select Committee.

Mark Meadows, a Republican Representative from North Carolina and chairman of the House Oversight Committee s Government Operations subcommittee, told The Hill that the stonetear posts are now under review:

> The Reddit post issue and its connection to Paul Combetta is currently being reviewed by OGR staff and evaluations are being made as to the authenticity of the post.
>
> and that the dates on the posts are troubling.
>
> If it is determined that the request to change email addresses was made by someone so closely aligned with the Secretary s IT operation as Mr. Combetta, then it will certainly prompt additional inquiry.
>
> The date of the Reddit post in relationship to the establishment of the Select Committee on Benghazi is also troubling.

The posts have since been deleted, but there are archived copies, such as this one from a popular thread on the Donald Trump-supporting subreddit r/The_Donald.

The archived post is the result of one forum member having urged others to

> ARCHIVE EVERYTHING YOU CAN!!!!

when the original posts were taken down.

Here s the text of the original Reddit post from stonetear, from 24 July 2014:

> Hello all- I may be facing a very interesting situation where I need to strip out a VIP s (VERY VIP) email address from a bunch of archived email that I have both in a live Exchange mailbox, as well as a PST file.
>
> Basically, they don t want the VIP s email address exposed to anyone, and want to be able to either strip out or replace the email address in the to/from fields in all of the emails we want to send out.
>
> I am not sure if something like this is possible with PowerShell, or exporting all of the emails to MSG and doing find/replaces with a batch processing program of some sort.
> Does anyone have experience with something like this, and/or suggestions on how this might be accomplished?

That request came the day after the House Select Committee on Benghazi had reached an agreement with the State Department on the production of Clinton s email records, according to an FBI report released earlier this month on the bureau s probe of her email use.

And this is the text of a post from stonetear made on 10 December 2014:

> Hello- I have a client who wants to push out a 60 day email retention policy for certain users. However, they also want these users to have a Save Folder in their Exchange folder list where the users can drop items that they want to hang onto longer than the 60 day window.
>
> All email in any other folder in the mailbox should purge anything older than 60 days (should not apply to calendar or contact items of course). How would I go about this? Some combination of retention and managed folder policy?

According to the FBI report, longtime Clinton aide and attorney Cheryl Mills had earlier that month asked that the email retention policy be shortened to 60 days because Clinton had decided she no longer needed access to messages older than that.

According to the report, Mills

> instructed [redacted] to modify the email retention policy on Clinton s clintonemail.com e-mail account

but that

according to [redacted] he did not make these changes to Clinton s clintonemail.com account until March 2015.

The New York Times has identified the redacted individual as more than likely being Combetta.

According to the FBI report, redacted/Combetta had a forehead-slapping moment in March when he realized he d failed to implement the new 60-day email retention policy:

[redacted] indicated he believed he had an oh sh*t moment and sometime between March 25-31, 2015, deleted the Clinton archive mailbox from the [Platte River Networks] server and used BleachBit to delete the exported .PST files he had created on the server system containing Clinton s emails.

The identity of the stonetear user is unconfirmed. Reddit users are pointing to the fact that an account on the online marketplace Etsy for a Paul Combetta has the same username stonetear , and the inactive website combetta.com is registered to the email address stonetear@gmail.com.

As of Monday, US News hadn t received any replies after having emailed that account.

According to The Hill, the committee looking into the matter has scheduled another hearing on the preservation of State Department records for Thursday.

Also, Oversight Chairman Jason Chaffetz, a Republican Congressman from Utah, last Monday issued a subpoena to the FBI, demanding the full case file from the email investigation.

He and other Republicans on the panel claim that the bureau has withheld summaries of interviews with witnesses and unnecessarily blacked out material from documents sent last month.

FCC Republicans Refused To Give Congress Net Neutrality Documents

An anonymous reader quotes a report from Ars Technica:

The two Republican members of the Federal Communications Commission have refused to give Congress documents needed to complete an investigation into the FCC’s net neutrality rule-making process, according to a lawmaker. "Your refusal to cooperate with the Committee’s request is unacceptable, it obstructs our investigation, and it prevents the Committee from having a complete or accurate understanding of the circumstances surrounding this rulemaking," U.S. Rep. Elijah Cummings (D-Maryland) wrote in a letter to FCC Commissioners Ajit Pai and Michael O’Rielly yesterday. There are "serious questions" about "Pai’s efforts to organize opposition to the proposed rule with outside parties," Cummings’ office said in a related press release. "Pai previously worked as associate general counsel for

Verizon, one of the major opponents of the open Internet policy, and he reportedly ’enjoys the support of conservative think tanks like the Phoenix Center, the Free State Foundation and TechFreedom,’" the press release said. O’Rielly wrote an op-ed on the net neutrality rules in 2014, but only after he "sought edits on [the] draft op-ed from three individuals outside the FCC with professional interests that could be affected by the rule," the press release said. The Republican lawmakers claimed that President Obama had "an improper influence" over the FCC’s decision and demanded documentation of all communication between FCC personnel and the White House, as well as calendar appointments, visitor logs, and meeting minutes related to meetings with the White House, plus all internal documents discussing the views and recommendations of the White House. They also asked for all documents and e-mails related to views of FCC personnel about the net neutrality proceeding.

A Cummings staff member told Ars that the "request has the backing of the full committee and all the enforcement mechanisms the committee has, including issuing a subpoena." The committee has schedule a hearing for September 27 on the status of outstanding document requests to different federal agencies, and could seek updates on the requests to the two Republican FCC commissioners at this hearing, a Democratic aide for the Oversight Committee also said.

Israeli Pentagon DDoSers Explain Their Work, Get Busted by FBI

Two Israeli men have been arrested for running a distributed-denial-of service-as-a-service site, after one seemingly claimed to attack the Pentagon.

Itay Huri and Yarden Bidani, released on US$10,000 bonds, were arrested following a tip off from the FBI, local news site TheMarker reports.

A Twitter account using Bidani’s name and handle tweeted last year that parts of the Pentagon site were down after a DDoS.

Their slick DDoS site vDos-s.com charged between US$30 and US$200 a month for DDoS attacks sold as legitimate network stress testing.

"We are not just another booter, we guarantee 10-50Gbps of UDP traffic per stress test using our DNS method, our high end dedicated servers can satisfy even the most power hungry customers," the pair wrote on their site.

VDos targeted 150,000 victims according to a stolen database provided to KrebsonSecurity lifted from the site by an anonymous security researcher who exploited a vulnerability.

That database revealed the actors’ identities along with details of paying customers.

The lifted document mentions victim sites including the UK’s Imperial College Model United Nations club, game site

GoodGame.co.uk, and anti-DDoS site Zare.com.

KrebsonSecurity says the booter site made some US$600,000 over the last two years.

The pair seemed to have tried to present the company as a legitimate stress testing service, rather than as guns for hire. Customers using the "legitimate stress testing company" are told they "are prohibited from stressing internet connections and/or servers that [they] do not have ownership of or authorisation to test".

Huri and Bidan even authored a technical paper [PDF] on DDoS last month, signing the document with their real names.

It’s OK for The FBI’s Fake Hacks To Hack Suspects’ PCs, Says DoJ Watchdog

No rules were broken when an FBI agent posed as a journalist to infect a criminal suspect’s PC with spyware, says a US watchdog. And the Feds can do it again, provided they get the undercover operation signed off by their higher-ups.

Way back in June 2007, 15-year-old Charles Jenkins used a Gmail account to send a bomb threat to Timberline High School, near Seattle, Washington, sparking an evacuation. Jenkins also flooded Timberline’s network with a 24-hour distributed denial-of-service attack for good measure.

Over the next few days, the teen sent a string of bomb claims to senior staff, using various Gmail accounts, triggering daily evacuations of the school. The messages were sent from IP addresses in Europe, suggesting the sender was working behind anonymizing proxy servers.

After the kid also created a MySpace page to boast about the threats, the Feds realized they were dealing with a classic attention-loving narcissist, and a cunning plan was concocted: a piece of spyware, dubbed a Computer and Internet Protocol Address Verifier (CIPAV), would be injected onto Jenkins’ PC to unmask him.

An agent, pretending to be an Associated Press editor, would send a message to the owner of the MySpace profile asking him for an interview. That message would contain a link to a webpage dressed up as a legit article. Hidden in that page is code that installs spyware on the machine, collecting information such as the public IP address, MAC address, details of the logged-in user, and so on. All this data is sent back to the FBI’s servers for processing.

The Feds followed standard procedure and were granted a search warrant by a court their application to the judge did not detail exactly how the operation would be carried out, simply that the CIPAV would be installed through an electronic messaging program from an account controlled by the FBI," and that it would "conduct a one-time search of the activating

computer."

Thus, FBI Special Agent Mason Grant messaged Jenkins with a link to a fake Seattle Times webpage asking if it was accurate and if the teen had any comment. Interestingly, even though the boy clicked on the link, the CIPAV failed to run due to undisclosed settings in his browser. In a followup Gmail chat with the undercover agent, Jenkins clicked on a link to some images, supplied by Grant, and the surveillance-ware was deployed. This coughed up his real public IP addresses, leading the FBI to his parents' home, where he was arrested and confessed.

The Feds' involvement in the case only came to light in 2014 when the EFF revealed Agent Grant had posed as an AP journalist. The newswire subsequently sued the federal government.

Now, the Office of the Inspector General at the US Department of Justice has this week published a report on the whole affair [PDF] and concluded that everything was done by the book although under policy changes in June this year, a similar operation today would require the green light from a string of senior staff.

That policy tweak was made following the revelations from the Jenkins' case, and provides clearer guidance for undercover agents impersonating news media professionals.

Here's the highlights of the report:

> We found that Department and FBI policies in effect in 2007 did not prohibit agents from impersonating journalists or from posing as a member of a news organization, nor was there any requirement that agents seek special approval to engage in such undercover activities. The only policies in effect at the time that might have required elevated consideration regarding the FBI s plans turned on whether the undercover activity involved a sensitive circumstance.
>
> We concluded, given the lack of clarity in the policy language, that making a determination whether a situation was a sensitive circumstance was a challenging one and that the judgments made by the agents were not unreasonable given the lack of clarity.

And finally:

> We also found that prior to the adoption of the new interim policy in June 2016, FBI policy would not have prohibited FBI employees from engaging in the undercover activities agents conducted during the 2007 Timberline investigation.
>
> The new interim policy, however, clearly prohibits FBI employees from engaging in an undercover activity in which they represent, pose, or claim to be members of the news media, unless the activity is authorized as part of an undercover operation.
>
> In order for such an operation to be authorized, the undercover application must first be approved by the head of the FBI field office submitting the application to FBIHQ, reviewed by the Undercover Review Committee at FBIHQ, and approved by the

Deputy Director, after consultation with the Deputy Attorney General.

In the end, a serial bomb hoaxer was collared and carted off after a mostly well-executed operation. But the use of spyware delivered through web links is problematic. Many things can go wrong imagine the chaos if the link was shared on social networks, infecting any number of systems, and if the shared payload fell into the hands of miscreants to reverse engineer and exploit privately.

This is on top of concerns that injected snitchware is potentially inadmissible in court due to the secrecy and security issues surrounding the code.

The AP, meanwhile, is furious.

"The Associated Press is deeply disappointed by the inspector general s findings, which effectively condone the FBI s impersonation of an AP journalist in 2007," Paul Colford, the newswire's director of media relations, said on Thursday.

"Such action compromises the ability of a free press to gather the news safely and effectively and raises serious constitutional concerns.

"Once again AP calls on the government to refrain from any activities involving the impersonation of the news media and we demand to be heard in the development of any policies addressing such conduct."

Why The Silencing of KrebsOnSecurity Opens A Troubling Chapter for The Net

For the better part of a day, KrebsOnSecurity, arguably the world's most intrepid source of security news, has been silenced, presumably by a handful of individuals who didn't like a recent series of exposØs reporter Brian Krebs wrote. The incident, and the record-breaking data assault that brought it on, open a troubling new chapter in the short history of the Internet.

The crippling distributed denial-of-service attacks started shortly after Krebs published stories stemming from the hack of a DDoS-for-hire service known as vDOS. The first article analyzed leaked data that identified some of the previously anonymous people closely tied to vDOS. It documented how they took in more than $600,000 by knocking other sites offline. A few days later, Krebs ran a follow-up piece detailing the arrests of two men who allegedly ran the service.

On Thursday morning, exactly two weeks after Krebs published his first post, he reported that a sustained attack was bombarding his site with as much as 620 gigabits per second of junk data. That staggering amount of data is among the biggest ever recorded. Krebs was able to stay online thanks to the generosity of Akamai, a network provider that providd a DDoS mitigation service to him for free. The attack showed no signs of waning as the day wore

on. Some indications suggest it may have grown stronger. At 4 pm, Akamai gave Krebs two hours' notice that it would no longer assume the considerable cost of defending KrebsOnSecurity. Krebs opted to shut down the site to prevent collateral damage hitting his service provider and its customers.

"It's hard to imagine a stronger form of censorship than these DDoS attacks because if nobody wants to take you on then that's pretty effective censorship," Krebs told Ars on Friday. "I've had a couple of big companies offer and then think better of offering to help me. That's been frustrating."

Until recently, a DDoS attack in excess of 600Gb was nearly impossible for all but the most sophisticated and powerful actors to carry out. In 2013, attacks against anti-spam organization Spamhaus generated headlines because the 300Gb torrents were coming uncomfortably close to Internet-threatening size. The assault against KrebsOnSecurity represents a much greater threat for at least two reasons. First, it's twice the size. Second and more significant, unlike the Spamhaus attacks, the staggering volume of bandwidth doesn't rely on misconfigured domain name system servers which, in the big picture, can be remedied with relative ease.

Instead, the attacks against KrebsOnSecurity harness so-called Internet-of-things devices think home routers, webcams, digital video recorders, and other everyday appliances that have Internet capabilities built into them. Manufacturers design these devices to be as inexpensive and easy-to-use as possible. Consumers often have little technical skill. As a result, the devices frequently come with bug-ridden firmware that never gets updated and easy-to-guess login credentials that never get changed. Their lax security and always-connected status makes the devices easy to remotely commandeer by people who turn them into digital cannons that spray the Internet with shrapnel. On Thursday, security firm Symantec cataloged 11 different families of IoT malware that do just that.

"The current IoT threat landscape shows that it does not require much to exploit an embedded device," Symantec researchers wrote in the report, which was headlined "IoT devices being increasingly used for DDoS attacks." "While we have come across several malware variants exploiting device vulnerabilities such as Shellshock or the flaw in Ubiquiti routers the majority of the threats simply take advantage of weak built-in defenses and default password configurations in embedded devices."

The growing supply of IoT malware is creating a tipping point in the denial-of-service domain that's giving relatively unsophisticated actors capabilities that were once reserved only for the most elite of attackers. And that, in turn, represents a threat to the Internet as we know it.

"The biggest threats as far as I'm concerned in terms of censorship come from these ginormous weapons these guys are building," Krebs said. "The idea that tools that used to be exclusively in the hands of nation states are now in the hands of individual actors, it's kind of like the specter of a James Bond movie."

Krebs said he has explored the possibility of retaining a DDoS mitigation service, but he found that the cost somewhere between $100,000 and $200,000 per year for the type of always-on protection he needs against high-bandwidth attacks is more than he can afford. For the past four years, he received pro bono help from Prolexic, which was later acquired by Akamai. Over that time, the service has defended KrebsOnSecurity against what he estimates are hundreds of attacks. The latest round has brought that relationship to an end. Krebs said he hopes to be back online later Friday with the help of a service he declined to discuss on the record. Still, he said, he’s not sure how long the new arrangement will last.

Of course, if a ragtag band of pseudo-hackers can disrupt KrebsOnSecurity, they can disrupt plenty of other sites, too. And this should concern not just the Googles, Apples, and Microsofts of the world but their everyday users as well. Krebs said the threat "screams out" for the kind of industry-wide collaboration that’s come together to counter previous threats, including the DNS spoofing bug researcher Dan Kaminsky disclosed in 2008, the Conficker worm that infected huge swaths of the Internet the same year, or the GameOver botnet from last year. Sadly, Krebs said he sees no signs of such cooperation now.

"Free speech in the age of the Internet is not really free," he said. "We’re long overdue to treat this threat with a lot more urgency. Unfortunately, I just don’t see that happening right now."

ACLU Is Launching A Campaign To Convince President Obama To Pardon Edward Snowden

Coinciding with the launch of Oliver Stone’s movie Snowden in select theaters this week, a coalition of civil rights groups are launching a campaign to convince President Obama to pardon NSA whistleblower Edward Snowden. Fusion reports:

The effort, which is organized by the ACLU, Amnesty International, and Human Rights Watch, will gather signatures from regular people and endorsements from celebrities. Snowden will speak by video link from Moscow at a press conference on Wednesday morning in New York, and an initial list of "prominent legal scholars, policy experts, human rights leaders, technologists and former government officials" in support of the cause will be released, according to a statement from the campaign. A presidential pardon would mean that Snowden could come home from Moscow, where he’s lived for the past three years, without the fear of being prosecuted. He currently faces federal charges of violating the Espionage Act and stealing government property, even though his disclosures led to reform of the wiretapping program by Congress.

Many Snowden supporters are hoping the movie Snowden, which opens in U.S. theaters on Friday, will spur support for a pardon. "I think the value of the movie is that it’s lsikely to reach millions of people who have not been paying close attention to Snowden or to the debate about surveillance and privacy," Snowden’s layer at the ACLU, Ben Wizner, told Fusion. "Those people will emerge from the movie more educated about

surveillance and with more positive attitudes toward Snowden."

EU Promises Free Wi-Fi to All

To expand its digital initiatives, the European Commission has planned to provide free wi-fi in all the public spaces across its member’s states within four years. The EU has a budget of 120 million set for this.

The commission will provide the set budget to subsidize the purchase and installation of Wi-Fi hotspots in 6,000 or more locations, but the provision of bandwidth and ongoing maintenance will be left to the local communities.

The project, WIFI4EU (Wi-Fi for EU) was announced by the president of the European Union’s executive body, Jean-Claude Juncker, in his annual state of the union address on Wednesday (September 14) which aims to put free Wi-Fi hotspots open to all EU citizens in parks, squares, libraries and other public buildings.

The hotspots will be open to all EU citizens, although given the budget it’s unlikely many of them will be able to get a signal without a long walk. In many towns and cities, people can already find free wi-fi on the High Street.

If local park or library already offers a paid Wi-Fi service, then the EU subsidy isn’t going to change anything. Projects that compete with a similar, existing private or public Wi-Fi offering will not be funded.

Juncker also announced that at least one city in each EU country will be deployed by the 5G mobile network by 2020.

This initiative would be crucial in rural areas where cellular networks are spotty or non-existent, and local organizations don’t always have the means to offer free WiFi hotspots. If a 120 million ($135 million) grant receives approval, communities would have access to the funds before the end of 2017.

Till 2025, EU has set some goals regarding the project which include minimum download speed of 100Mbps for all European households, minimum download and upload speeds of 1GBps for all hospitals, administrations and other public services reliant on digital technologies and uninterrupted 5G access for all major roads and railways.

The commission hopes to serve thousands of connections daily. If one connection represents one user, its goal is to connect almost one-tenth of the EU’s population each day.

However, there is a doubt if the public would benefit or not as European officials have been struggling to deliver an earlier promise to abolish mobile roaming fees.

The EU is also committed to its promises of erasing borders for media services, too. It wants to make content accessible across

the Union so that the content is not limited in one s home country. People can watch German Netflix shows while visiting France, for example. They could also buy pay-TV movies and similar material from other countries, some of which might well be less expensive than it is at home. Broadcasters would still have control over whether or not their content is available in other countries.

The new pledges may not apply to the UK because it may have quit the EU before the end of the decade.

With this proposal, there are copyright changes which are disturbing Google. The proposal would require better data sharing and transparency for creators, but it would also give press publishers rights that ensure they get a "fair share" of revenues for material they post online. This law is similar to ones in Germany and Spain which ask search engines like Google to pay up when they show an article snippet in their results. The EU contends that this is necessary to make sure writers are "paid fairly," but Google unsurprisingly objects. It believes that the German and Spanish laws "failed," and that these demands for payment ultimately hurt publishers by giving web users fewer reasons to click through to an article.

Moreover, the proposal requires that content uploaded on YouTube is copyrighted. While this does include "content recognition technologies" (possibly a reference to YouTube’s Content ID), Google is worried that the measure would require screening content before it goes public, which would demand far more work and investigation.

The proposal needs to clear both the European Parliament and individual governments to go forward. It may take a long time before the initiative takes effect without any significant changes. The initiative if applied would give a different digital landscape to entire Europe but there’s a concern that Google and others like it might scale back their European presence rather than make the effort to comply with new copyright laws.

Twitter s New, Simpler Rules for Character Counts in Tweets Go Live

Did you hear? Twitter would like you to know that its service is now easier to use, thanks to a series of rule revisions announced in May, which have just gone live. Starting today, Twitter is cutting down on what counts towards your 140 characters. As a refresher, that means media content like photos, videos, GIFs, polls and Quote Tweets no longer eat into your character count. Links still do, however.

As you may recall, Twitter first announced all these changes earlier this year, but delayed their rollout to give the developer community time to adapt.

Along with changing what counts towards the 140 characters, Twitter also announced other tweaks at the same time like

ditching the .@ format, for example. This convention came about when people wanted to send tweets that began with an @username to their entire audience. Something of a user-generated hack, the period . circumvented Twitter s restrictions on which tweets appear in followers Timelines.

Twitter likes to tout all these changes as a means of simplifying its service   something it s doing in an effort to appeal to new users who find the intricacies of using Twitter confusing. Twitter has seen its user growth stagnate, which has been worrying Wall St. and leading to rumors that the service is looking for an acquirer.

The goal with its departure from the 140 characters   Twitter s defining feature from day one   is to make the service easier to use.

And it s just so much easier, right?

Right?

In case you need a cheat sheet, here s a summary of Twitter s newer, simpler rules, including all those announced alongside the character count changes back in May. (See below)

(Note that the RT and QT changes were shipped a few months ago, while the @mentions and .@ changes are still forthcoming.)

    You can only use 140 characters when composing a tweet. (Simplicity at its finest!)
    Oh, except when you re posting non-text content like videos, GIFs, pictures and polls? ?those don t count toward your 140 characters.
    But links still do.
    Quote tweets don t though. Because even though they re text, they re like, old. Old stuff doesn t count, only new stuff does .I think.
    ANYWAY, @mentions in replies won t show anymore in the tweet? ?they re like, in the header in the user interface or something.
    Yep, so these @mentions won t count toward the 140 and you can mention up to 50 people.
    But if you want everyone to see your @reply, Twitter wants you to retweet yourself.
    Right? ?you can do that, Twitter says!? ?retweet yourself.
    And quote yourself.
    If you don t do that, not everyone will see your @reply.
    Well, I mean if you write a new tweet that starts with an @username that s like, not technically a reply. So it will been seen by everyone.
    So actually, Twitter is not really changing the rules for who can see your replies? ?because new tweets that begin with @username mentions aren t really replies. The only people who will see your @ reply in their timeline are those who follow you and the person you re replying to. Like before!
    Which means, I guess, if you want everyone to see your tweet even when they don t follow both parties you could still use the period before the @username to make that happen .? Hold on, I m getting confused
    But now you can retweet yourself so I guess Twitter would

prefer you did that instead of using the dot @username thing? So this whole change is more of a suggestion, I guess?

Oh, and use the native retweet if you retweet yourself no one writes RT anymore.

Or MT. No one does that. That was dumb.

But when @usernames are mentioned in tweets, they still count toward your 140 characters like regular words do. (Just not when you re replying to those @usernames and the @usernames are auto-populated).

I mean, really, isn t this so much better than oh, I don t know just displaying the first 140 characters, then hiding the rest behind a click?

And isn t this feature set just hugely in demand, even more so than an edit your tweet button or some sort of legitimate product built in response to the widespread cyberbullying and trolling that takes place on Twitter you know, something like what Instagram just launched?

I mean, I don t hear anyone asking for these things

Anyway new ways to reduce character count. Yay.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.